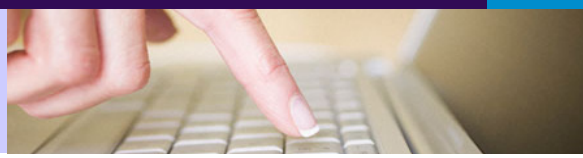
Security Awareness News

January 2008



My 2008 Resolution: To Get Into Good Security Habits

We hope you all had a happy and safe holiday season. As we enter 2008, each of us also hopes for prosperity, health and security. Achieving those goals is in large part up to us individually.

Many of us probably made New Year's Resolutions at the stroke of midnight or in the days surrounding the New Year. Some of us perhaps resolved – with the best of intentions – to quit smoking, or perhaps to diet or exercise more, all in the name of our personal health.

We may have vowed to spend less or clean up credit card debt, with the goal to improve our personal finances in the coming years. Some folks will plan to attend more of their kids' ball games, or volunteer at the local shelter more often. All good resolutions, for sure.

But how many of you made a New Year's Resolution about security? Did you even think about the possibilities? Well we have done some of that for you and here are few to consider as we enter 2008, destined to be, by all reports and accounts, even worse security-wise than 2007.

My Work-Related New Year's Security Resolutions for 2008

1. I will find those old documents HR gave me when I got hired and review them.
2. I will make sure my passwords on all systems meet company policy and guidelines.
3. I will find and completely review our corporate security policy.
4. I will learn and make note of, whom to call, e-mail or contact in case of a physical or cyber emergency.
5. I will read at least one information security book this year. (Non-fiction, of course.)
6. I will never, ever, open an e-mail attachment unless it has been scanned by approved software.
7. I will not answer e-mails offering get rich quick schemes, scams, or others requiring my immediate attention from people I do not know.
8. I will participate in security briefings, training, and tests in order to make me more of a secure user.
9. I will learn to act as a human firewall and human intrusion detection system in order to help the security of our company.
10. If I suspect any security violation of our company data or facilities, I will report it immediately.

My Personal New Year's Security Resolutions for 2008

1. I will get a paper shredder for home, and be more alert about personal data I throw into the garbage.
2. I will set up 'User' non-admin ac-

Continued on p. 2

Who Ya Gonna Call?

Need to Report Something?

Contact Security, your IT manager, or Help Desk immediately.

Good security comes from timely response!

Continued from p. 1

counts for everyone in the family.

3. I will check my paper and on-line statements from banks, credit cards and utilities diligently, to avoid becoming the victim of identity theft.
4. I will regularly clean up my personal computer(s) with all patches, upgrades and new security tools to meet the new threats.
5. I will make sure my high-speed connection has a firewall that keeps hostile traffic from coming into my house and from sending out our personal information.
6. I will not click through on e-mails allegedly from my bank, credit card, PayPal or other account warning me of fraud. I will only use my normal access methods, because the others are probably frauds.
7. I will learn to use a 'mouse-over' to see the real URL when I am asked to click-through, especially when I am on unfamiliar or potentially untrustworthy web sites.
8. I will subscribe to at least two security news feeds so I can stay on top of the latest threats to my computers and electronic life.
9. I will talk with my kids and family regularly to discuss the security threats from the Internet as well as ethical and legal behavior. I will, finally, really install parental monitoring software to see what my kids are doing on-line.
10. I will increase my level of security awareness to protect my family and our personal assets all year long.

Hopefully, these short lists of Resolutions will trigger additional ideas of your own, too. Not one of these Resolutions is particularly difficult, as is true with all security. It's about doing and being aware of lots of little things, so when they are added up, your personal security and our company security is measurably better.

If you think of a few of your own Resolutions that would benefit others, share them! Security Awareness is a TEAM EFFORT!

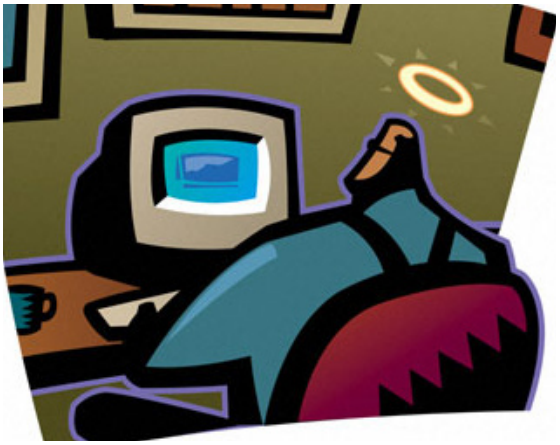
Let's All Have a Successful, Safe and Secure 2008!

The Dream Security Aware User

Companies want their users to be security aware.

We also want our users to report security events. We want them to talk to us. We want communication so that a security event does not escalate out of control. But we also do not want users taking security and highly technical issues into their own hands at work. We have IT and Information Security Departments to handle things according to well-established policy and procedure.

Today, help desk pros increasingly view their job as one of teaching, giving users confidence to solve some of their own problems, to experiment, and to try new things.



Some people might think IT help desk pros would define their Dream User as the one they never hear from. But you'd be wrong. While IT help desk experts may have slightly differing opinions on the more negative user archetypes they see, a recent study showed they were in agreement about the 'user of their dreams.' Here we have summarized some of their comments:

- If we never hear from someone, that probably means they're fighting through something that's ruining their productivity.
- An experienced remote user called after encountering an error message while replacing a video card. She wanted to know why that happened. Her desire for knowledge was admirable.
- Our favorite user is a proactive user. If people aren't calling, that probably means they're getting frustrated.
- Our Dream User is someone who actually listens to what we say.
- We don't mind if people call a lot. Ignorance is fine, but listen to what we are telling you and follow through. Take notes if you have to, and don't be afraid. Be as receptive and respectful as we've been to you.

Users can best help IT and security folks by being accurate. That indeed may mean writing down notes, even things you don't understand. The more information we have, the better.

Also, keep in mind that a time-line helps. Think of any cop show on TV and they all develop time lines. Something like this might work:

1. Your computer was fine two days ago.
2. Then A.B.C. happened yesterday in the morning.
3. Then D.E.F. happened when you got back from lunch.
4. And this morning, nothing worked at all.

By telling us what, when and where, you make our jobs easier, we are more effective, and we can solve problems more efficiently.

Kicking Bad E-Mail Habits Into Good E-Mail Habits

E-mail has the honor of holding three places in ubiquity:

1. It is how the vast majority of business is communicated.
2. It is how the vast majority of businesses are infected with hostile software.
3. It is how the vast majority of businesses lose productivity.

E-mail can be an addiction, and any addiction can easily lead to mistakes, and in our case, security relevant errors that can affect our entire company. We all need it, every day, but there are some tricks that can help security and can improve your productivity.

• One bad habit is hoarding e-mails, unorganized, in the inbox. Some people actually have thousands of e-mails held in a single directory, which means they are no longer in control of their e-mail data. Running through e-mails quickly to dispose of the unneeded ones can often cause a usually 'security aware' user to open something he otherwise wouldn't. "Noodling" through masses of e-mails becomes a time waster and security risk. Handle e-mail regularly, as often as necessary to avoid overwhelming numbers of messages you might carelessly race through.

• Good security policies should also reflect some recognized and efficient methods for storing large numbers of e-mails. Make sure you know company procedures and recommendations for organizing and backing up your e-mail files.

• E-mail also causes interruptions, which can be a security problem. When an e-mail arrives and the alert sounds, some people immediately check to see who has written to them. This distracts them from other tasks, some of which can easily have serious security implications to our company. Consider turning off automatic download, and only "Get Messages" when you are not doing several other things. But do allow enough time throughout the day to sort through them. Make sure you know company e-mail policies.

• Sending an e-mail to too many people is a waste of time, but can also unintentionally spread hostile code if you do happen to get infected. Imagine going into a party with 100 people during the cold and flu season. You or someone else at the party could have a viral infection, but not know it yet. This would be a good time to avoid shaking hands and kissing cheeks. Perhaps you should think about this before sending mass copies of e-mails. Limiting exposure is a good thing. And of course, when at work, follow all company e-mail policies.

Treat the use and organization of e-mail as a security relevant duty in addition to making sure it has been scanned for viruses. The bad guys know that many people get careless about their e-mail habits and use the inbox as a massive repository for data. So, they send hostile e-mails with old dates that will appear way down the list in your inbox. While noodling, you come across something old and interesting and you … <Click>, when you shouldn't.

Just another piece of valuable security awareness that could help you avoid problems along the way.

COMING NEXT MONTH!

Corporate Crime & Espionage

1. The Storm is the biggest computer in the world. You will see how and why you must defend against it.

2. The figures are in: Spam and Bots are all about the money. We'll show you what's what.

3. There is more on-line spying than you can imagine, often done by governments themselves.

4. Are you a victim? Are you high profile? Is your company? What special precautions do you need to take?

Did You Know?

Accoding to security experts, the biggest security vulnerabilities in 2007 were browser exploits, data breaches and the ever-lurking spyware. But 2008 will have a few new security surprises for us including iPhone hacks galore and P2P network spammers. Cisco also released its first report on the global state of security, listing professional hackers as one of the biggest vulnerabilties of 2008!